AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A copy protection method for digital media, the method comprising the steps of:

(a) encrypting an original media data set with a media key having a symmetric algorithm and encrypting said media key with a public key of a compliant device;

(b) delivering said encrypted media data set and said encrypted media key to a compliant playing device, wherein said original media data set includes an owner watermark containing an owner identification and owner copy-control information for the media data set;

(c) decrypting said delivered media key with a private key of said playing device;

(d) decrypting said delivered media data set with said decrypted media key;

(e) adding a player watermark to said decrypted media data set if said decrypted data set is not marked with at least "free copy", said player watermark containing a player identification of said playing device and player copy-control information, wherein said player copy-control information is derived from said owner copy-control information; and

(f) encrypting said watermark-added media data set with said decrypted media key and encrypting said decrypted media key with said public key of said compliant device, and passing said encrypted watermark-added media data set and said encrypted media key to a recording device without a compliance test;, or ~~(g)~~ performing a compliance test with a displaying device and if said compliance test is successful, passing said watermark-added media data set and said decrypted media key to said displaying device.

2. (Previously Presented) The method of claim 1, wherein said public key corresponds to an asymmetric algorithm.

3-10. (Canceled)

11. (Currently Amended) A copy protection method for digital media, the method comprising:

(a) receiving an encrypted media data set, a control information, and an encrypted media key, wherein the encrypted media data is generated by an original media data set with a media key and the encrypted media key is generated by encrypting said media key with a public key of a compliant device, wherein the control information includes owner identification of

media data set and a copy control information to indicate whether a copy of the media data set permitted;

(b) decrypting said received media key with a private key of said compliant device, and decrypting said received media data set with said decrypted media key;

(c) adding a device information to the media data set to indicate an origin of the media data set, said device information including a device identification and copy-control information, wherein said copy-control information is derived from said owner copy-control information; and

(d) outputting said media data set to which the device information is added, to an external device, wherein said outputting comprises (e) if said external device is a recording device, encrypting said media data set with said decrypted media key ~~prior to said~~ and outputting without a compliance test, and (f) if said external device is a displaying device, performing a compliance test with said displaying device ~~prior to said~~ and outputting without encrypting.

12. (Canceled)

13. (Previously Presented) The method of claim 11, wherein said compliance test is performed through an authentication process between said compliant device and said displaying

device wherein said step (d) outputs said media data set to which the device information is added only if said authentication is successful.

14.-20. (Canceled)

21. (Previously Presented) The method of claim 1, wherein said player copy-control information is set to "for display only" if said media data set is passed to said displaying device.

22. (Previously Presented) The method of claim 11, wherein said player copy control information is set to "for display only" if said media data set is passed to said displaying device.

23. (New) A copy protection system for digital media, the system comprising:

a receiving unit configured for receiving an encrypted media data set, a control information, and an encrypted media key, wherein the encrypted media data is generated by an original media data set with a media key and the encrypted media key is generated by encrypting said media key with a public key of a compliant device, wherein the control information includes owner identification of media data set and a copy control information to indicate whether a copy of the media data set is permitted;

a decrypting unit configured for decrypting said received media key with a private key of said compliant device, and decrypting said received media data set with said decrypted media key;

a watermark adder configured for adding a device information to the media data set to indicate an origin of the media data set, said device information including a device identification and copy-control information, wherein said copy-control information is derived from said owner copy-control information; and

an output unit configured for outputting said media data set to which the device information is added, to an external device, wherein said output unit encrypts said media data set with said decrypted media key and outputs without a compliance test if said external device is a recording device, while said output unit performs a compliance test with said displaying device and outputs without encrypting if said external device is a displaying device.

24. (New) The system of claim 23, wherein said compliance test is performed through an authentication process between said compliant device and said displaying device, wherein said output unit is configured for outputting said media data set to which the device information is added only if said authentication is successful.

25. (New) The system of claim 23, wherein said player copy-control information is set to "for display only" if said media data set is passed to said displaying device.